

All Posts

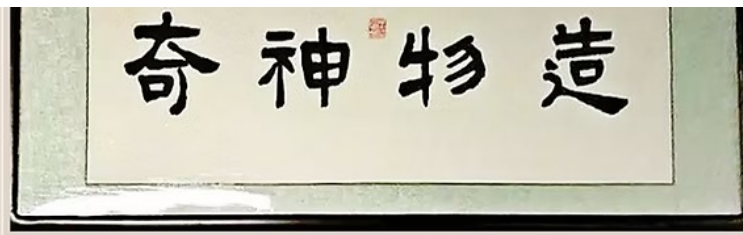


Trevor Alexander Nestor · 7 days ago · 3 min read



How China is Cracking Postquantum Cryptography

Updated: 1 day ago



logical



The central goal of professor Jinxing Zhang's research lab is the pursuit of emergent quantum phenomena and functionalities in strongly correlated oxides with artificially engineered time-reversal and/or space-inversion symmetry break.

Positions for post-doctoral scholars and Graduate students are available. Ambitious undergraduate and visiting students are also welcome. Please directly contact professor Jinxing Zhang via jxzhang@bnu.edu.cn

University, No.19, Xijiekouwai Street, Haidian District, Beijing, P.R. China.

(+86) 010-58801886, -----Email: jxzhang@bnu.edu.cn

Let's Chat!

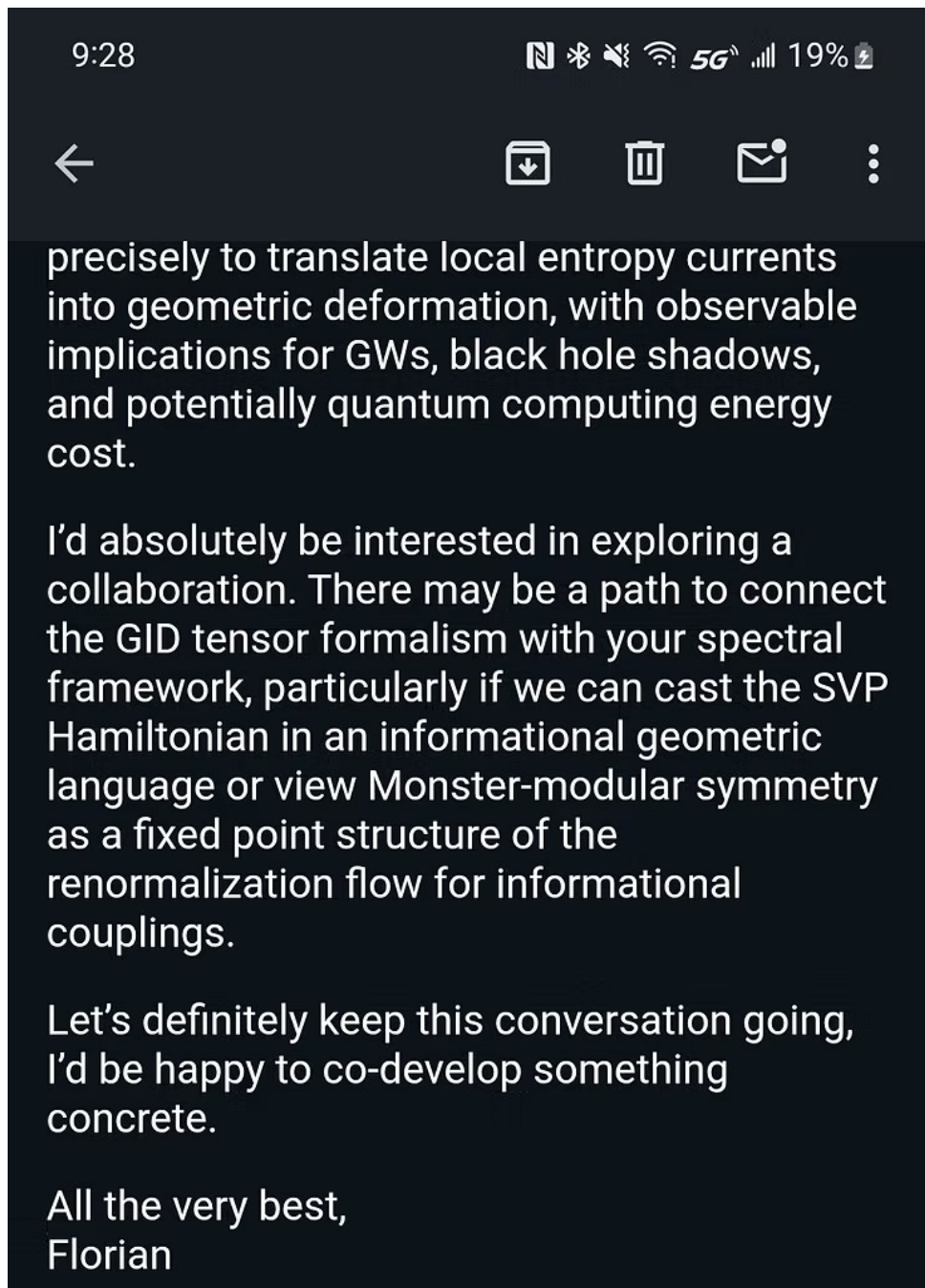
<https://link.springer.com/article/10.1134/S0021364023602683>

This month I'm visiting a lab in Beijing that claims to be investigating novel physics that would be capable of breaking the NP-Hard shortest vector problem in postquantum lattice cryptography - NIST's new standards (FIPS 203 and FIPS 204) that were supposed to safeguard against quantum attacks. Any breach of this would be catastrophic to banks, cryptocurrencies (like ICP), governments, and institutional stability. New physics may be required to breach it.

<https://zhanglab.bnu.edu.cn/>

https://harvest.aps.org/v2/journals/articles/10.1103/PhysRevLett.81.3992/fulltext?utm_source=chatgpt.com

Previously, I've had peer review articles on the theoretical feasibility of breaking postquantum cryptography published and cited by leading researchers (even at the World Economics Forum) on this topic -

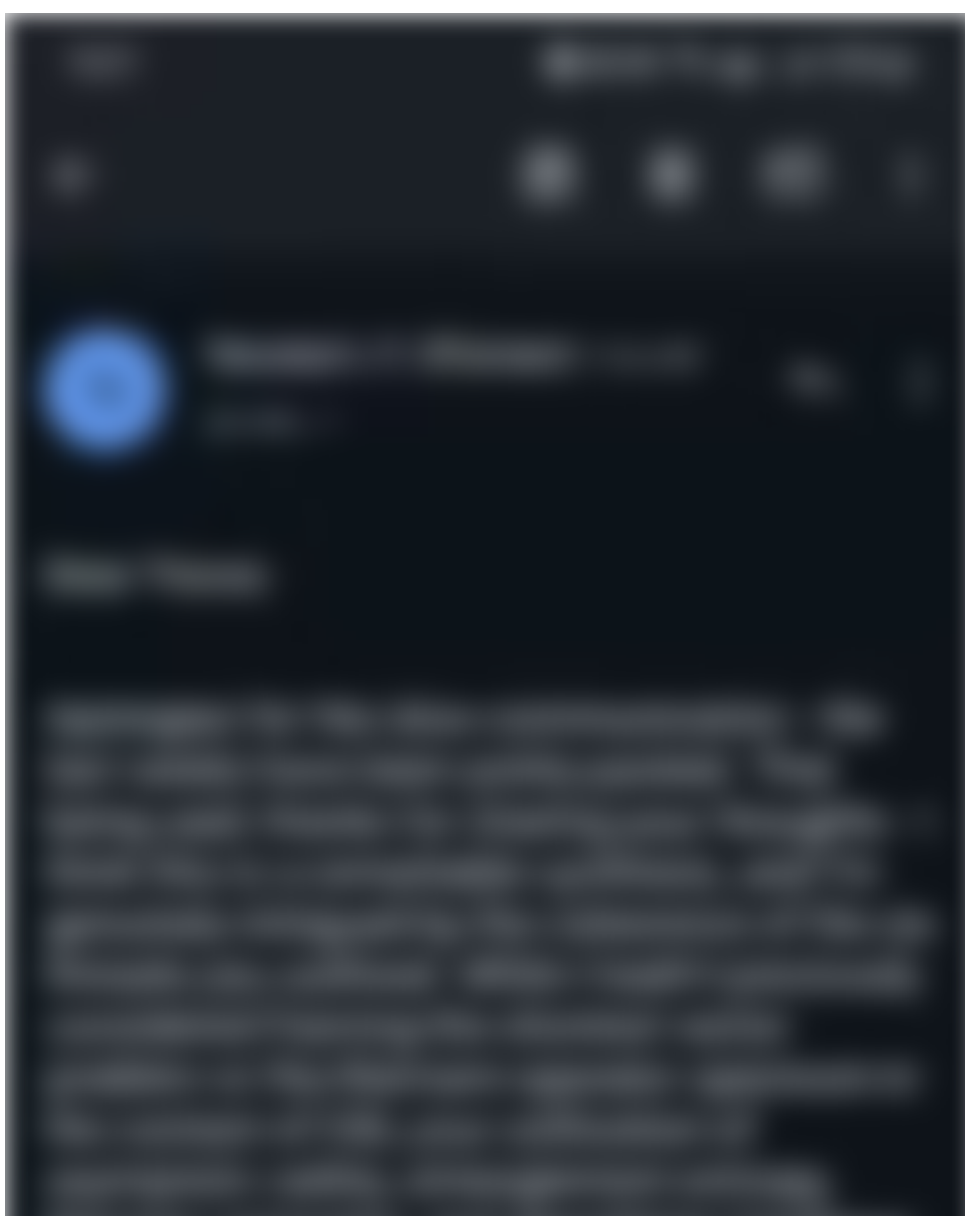


Prof. Dr. Florian Neukart
M: f.neukart@liacs.leidenuniv.nl

Web profiles:
[Linkedin](#)
[University of Leiden](#)

From: Trevor Alexander Nestor
<trevornestor@berkeley.edu>
Sent: Monday, May 19, 2025 4:57 PM

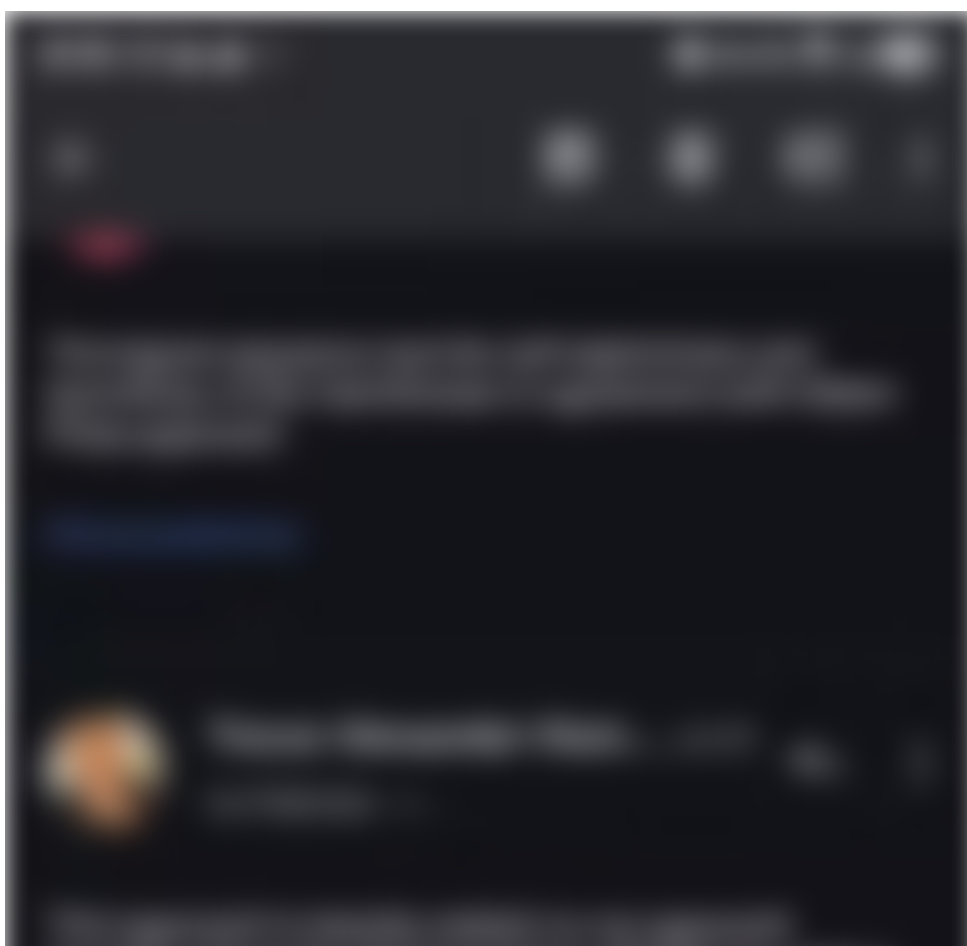
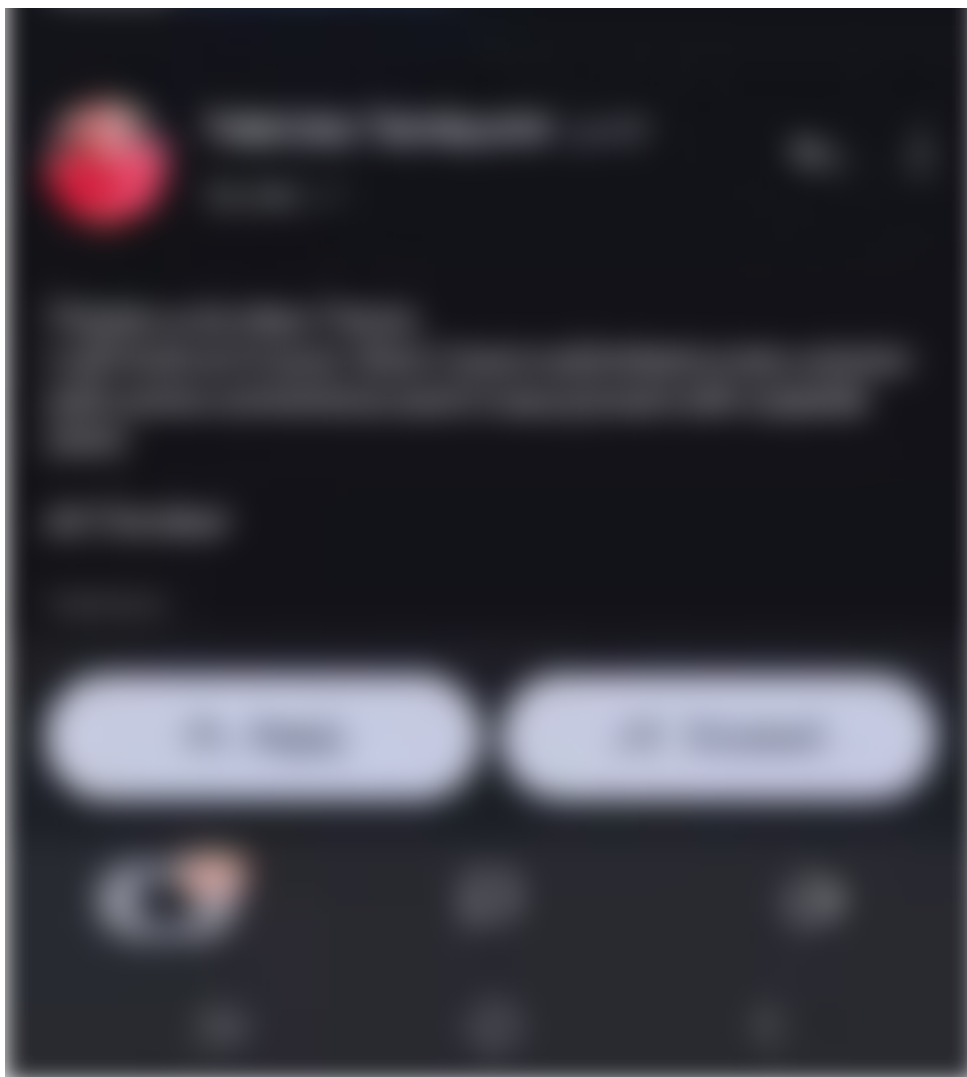
[Show quoted text](#)

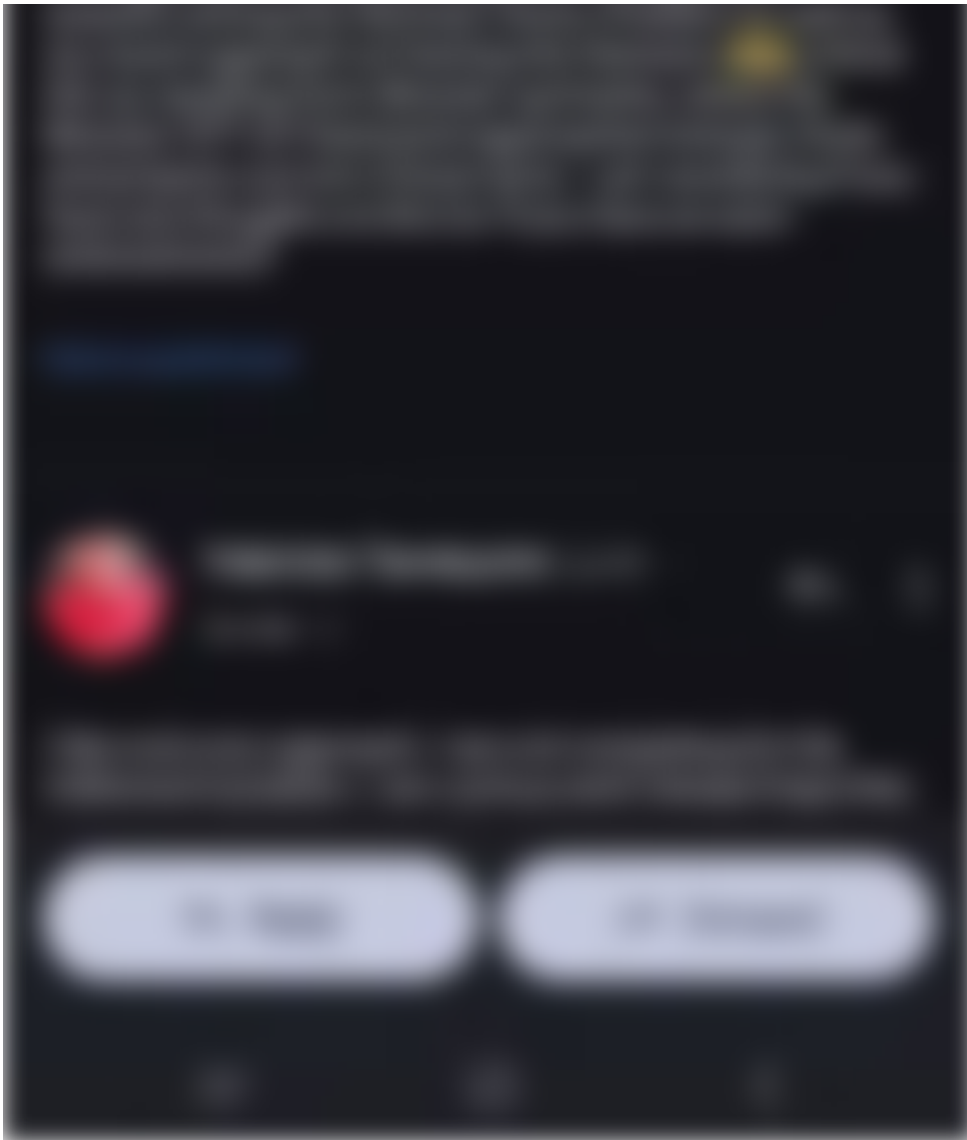


[illegible]

Name		Date	
1. Introduction			
2. Objectives			
3. Methodology			
4. Results and Discussion			
5. Conclusion			
6. References			
7. Appendix			
8. Summary			
9. Conclusion			
10. References			
11. Appendix			
12. Summary			
13. Conclusion			
14. References			
15. Appendix			
16. Summary			
17. Conclusion			
18. References			
19. Appendix			
20. Summary			
21. Conclusion			
22. References			
23. Appendix			
24. Summary			
25. Conclusion			
26. References			
27. Appendix			
28. Summary			
29. Conclusion			
30. References			
31. Appendix			
32. Summary			
33. Conclusion			
34. References			
35. Appendix			
36. Summary			
37. Conclusion			
38. References			
39. Appendix			
40. Summary			
41. Conclusion			
42. References			
43. Appendix			
44. Summary			
45. Conclusion			
46. References			
47. Appendix			
48. Summary			
49. Conclusion			
50. References			
51. Appendix			
52. Summary			
53. Conclusion			
54. References			
55. Appendix			
56. Summary			
57. Conclusion			
58. References			
59. Appendix			
60. Summary			
61. Conclusion			
62. References			
63. Appendix			
64. Summary			
65. Conclusion			
66. References			
67. Appendix			







it was my undergraduate professor fields medalist Dr. Richard Borchers at UC Berkeley who first got me interested in this topic, as his research into lattice maths and frontiers into quantum gravity research is directly applicable. I'm here to report that to hand the universe any class of ostensibly uncrackable encryption is much like to hand a lock to the grand lock and keymaker and claim that it cannot be unlocked - something quite hubristic to suggest. Indeed, we know from physics even with the black hole information paradox - the universe's most extreme one way information gate - unitarity should be preserved.

<https://ipublishing.org/index.php/ipil/article/view/171>

Interestingly, the field of physics known as Majorana physics which they are studying at Microsoft could be the answer - which may also be related to the mechanism by which the brain generates consciousness - an NP-Hard problem - classifying the problem as out of reach from our current computational technology and future quantum computing technology. The new physics required lies at the intersection of classical physics (nonlinear dynamics) and quantum field theory - quantum gravity - and I've got a preprint out that is currently under peer review at a top journal on this topic.





My first paper on this topic was published and second is out for peer review.



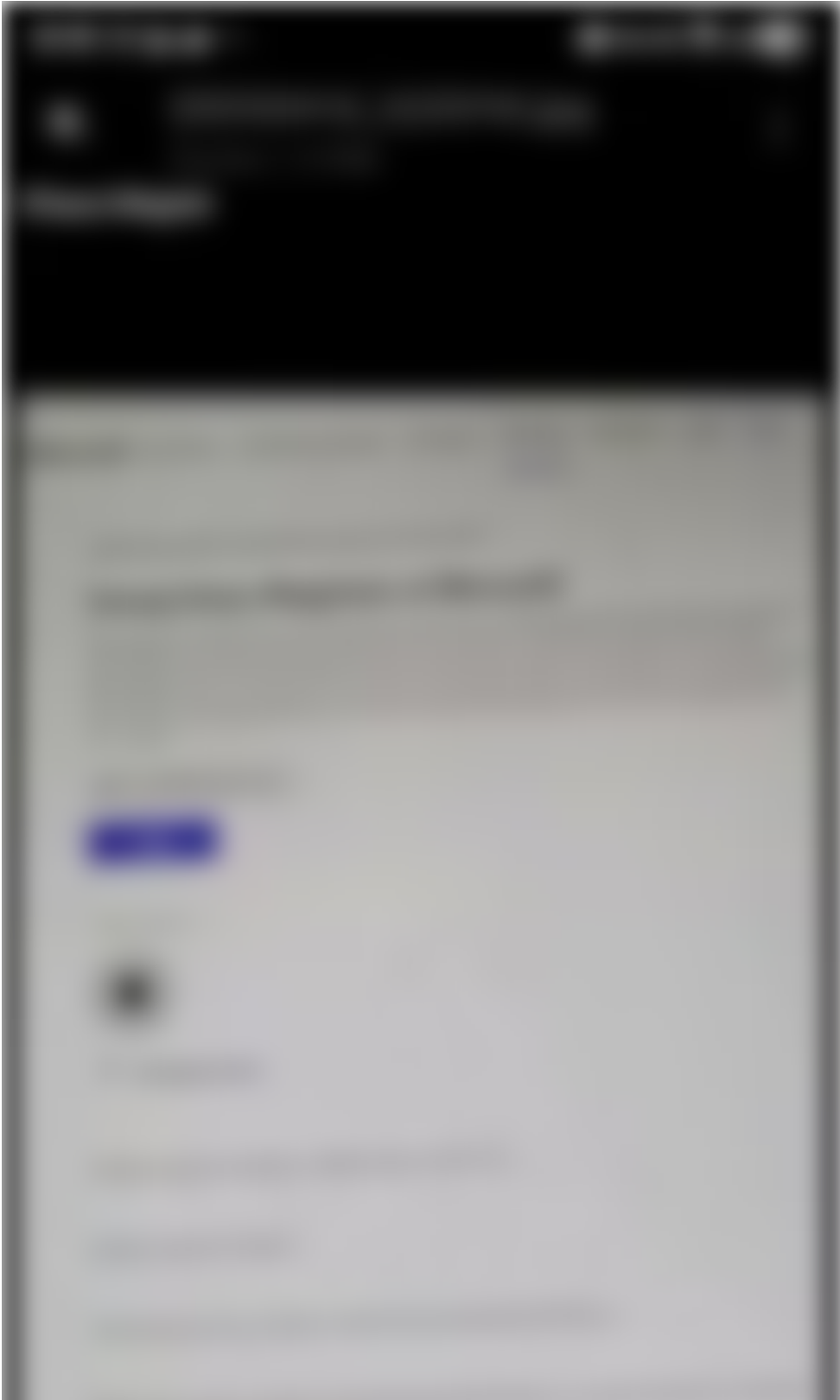
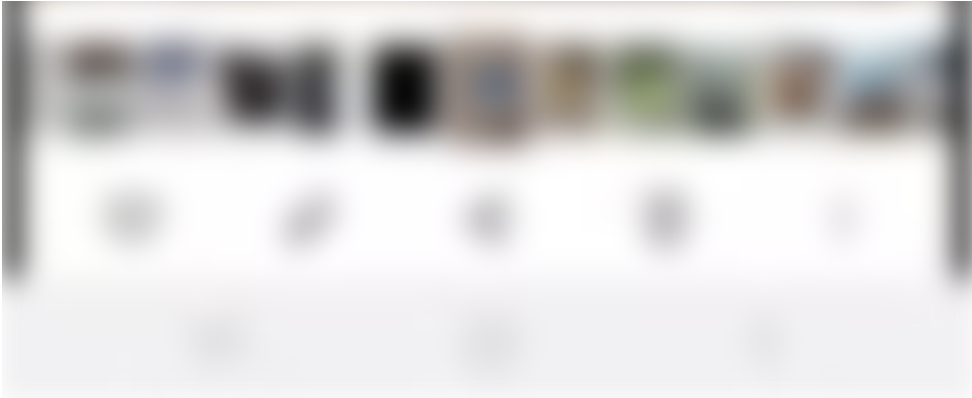
It sure is a shame that Microsoft wanted to wrongfully terminate me from the company so that I no longer have any reason to care about sharing all of this publicly (they can't even get their Majorana One chip to work after lying to their shareholders about it). I will provide future updates as I retain further information.

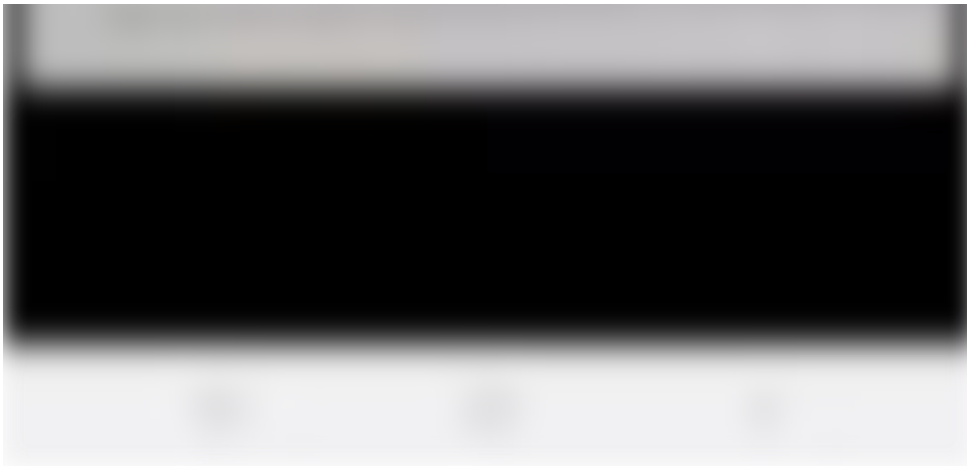




The cryptography subreddit appears to be astroturfed.







The idea for this postquantum cryptography is that this new cryptography is based on what are known as lattice problems. You have a "high dimensional" lattice (essentially a sort of hierarchical matrix where the "extra dimensions" are complexity abstractions rather than physical dimensions) - finding the shortest vector in these problems under random reductions is known to be a problem that is NP-Hard - a classification of computational complexity that is known to be intractable for our current and likely emerging quantum computers - even with prime factorization speedups like Grover's algorithm.

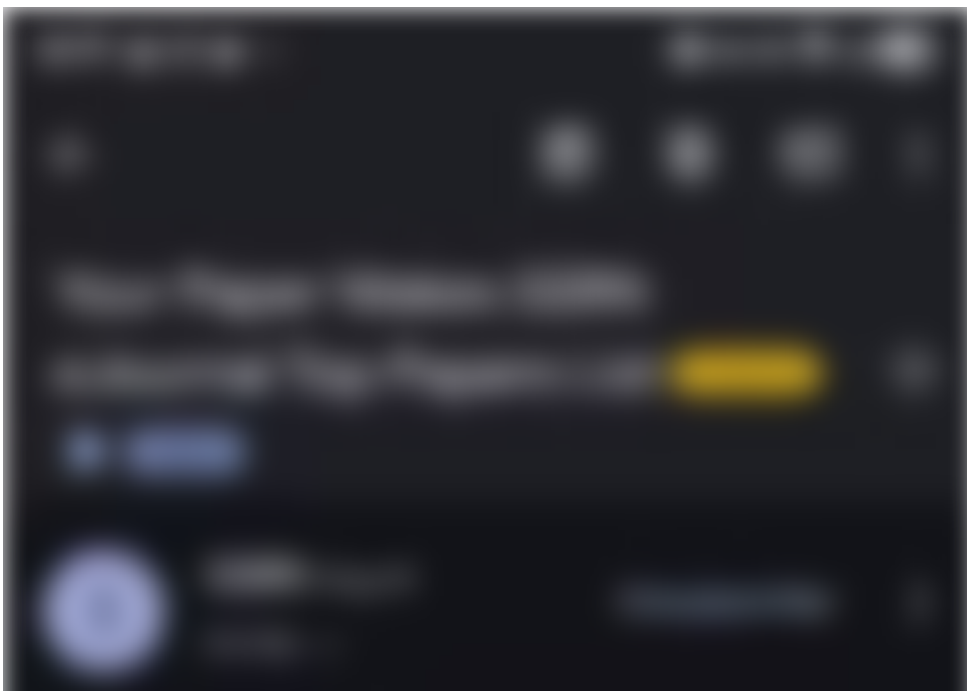
<https://scispace.com/papers/the-shortest-vector-problem-in-l2-is-np-hard-for-randomized-1w5emy4lda>

https://scholarworks.utep.edu/cgi/viewcontent.cgi?article=2363&context=cs_techrep

<https://thequantuminsider.com/2025/04/30/new-study-suggests-gravity-may-be-an-optimization-process-in-a-computational-universe/>

<https://link.springer.com/article/10.1007/s10909-022-02694-z>

With new theories of gravity, one might actually be able to develop a quantum gravity computer - where gravity itself might collapse evolving wavefunctions of particles traversing the lattice space to the shortest vector using spectral methods. What's interesting is that this approach may also be the mechanism by which consciousness and perceptual binding themselves are generated (so perhaps consciousness itself is an NP-Hard problem - which would certainly explain why current AI technology as interesting as it is, is not truly "sentient").





In the theory of Loop Quantum Gravity, spacetime is described by what are called "spinfoam networks." I've discussed in previous articles that the brain's neural networks themselves, if Dr. Penrose's theory about consciousness is correct, may actually be the physical spinfoam networks described by the theory.

<https://www.sciencedaily.com/releases/2014/01/140116085105.htm>

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5373371

[!\[\]\(e2376d476d06eb31946dc01a69a4403a_img.jpg\)](#) [!\[\]\(bbb3388d591ef640dd8a8c4262f2866a_img.jpg\)](#) [!\[\]\(ef6e697e79b33cfafe8ba6744dc11bd6_img.jpg\)](#) [!\[\]\(36a26e5b369c5d231b75de2efc184e39_img.jpg\)](#)

143 views 0 comments

1 

Microsoft's Study on Jobs AI
Can Replace is a White...

👁 154

💬 0



Living like a King Abroad
Cost Less than Rent in the...

👁 23

💬 0

1 ❤

What I Learned at the
Temple of the Reclining...

👁 4

💬 0

1 ❤

My Story

Get to Know Me

I have been on many strange adventures traveling off-grid around the world which has contributed to my understanding of the universe and my dedication towards science advocacy, housing affordability, academic integrity, and education funding. From witnessing Occupy Cal amid 500 million dollar budget cuts to the UC system, to corporate and government corruption and academic gatekeeping, I decided to achieve background independence and live in a trailer "tiny home" I built so that I would be able to pursue my endeavors.

[Read More](#)

Contact Information

Information Physics Institute
University of Portsmouth, UK

PO Box 7299
Bellevue, WA 98008-1299

First Name

Last Name

Email *

Subject

Leave a message

trevornestor@berkeley.edu

trevornestor@microsoft.com
tnesto1@lsu.edu
itstrevor@gmail.com
contact@trevornestor.com
trevor.nestor@informationphysicsinstitute.net
<https://www.linkedin.com/in/trevornestor>
1 720-322-4143



Submit